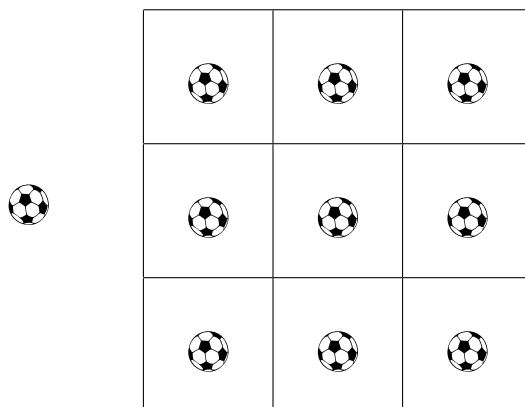


Dirichletov princip in paradoks rojstnega dneva

Primož Moravec
Fakulteta za matematiko in fiziko
Univerza v Ljubljani

19. maj 2017

Dirichletov princip ni nič drugega kot enostavno dejstvo, ki ga lahko formuliramo na naslednji način: *Če v n škatel razporedimo $n + 1$ žogic, sta v eni škatli vsaj dve žogici.* Na prvi pogled nič posebnega, toda to načelo ima številne uporabe v matematiki. Prvič se je pojavilo v literaturi z delom Dirichleta (1805–1859) v teoriji števil, zato tudi nosi njegovo ime. Prispevek o Dirichletovem principu je že izšel v Preseku [1] pred 30 leti.



Slika 1: Deset žogic in devet škatel.

Tudi v tem članku bomo prikazali nekaj uporab, na koncu pa bomo problem razporejanja žogic v škatle pogledali še z drugega, verjetnostnega, zornega kota.

Oglejmo si nekaj osnovnih primerov. Recimo, da imamo skupino 367 ljudi. Potem med njimi obstajata vsaj dve osebi, ki praznujeta rojstni dan na isti dan. Podoben sklep pokaže, da med poljubnimi štirimi naravnimi števili obstajata dve, ki imata isti ostanek pri deljenju s 3. Poleg tega očitno velja nekoliko splošnejša različica Dirichletovega principa, ki se glasi: Če v n škatel razporedimo $kn + 1$ žogic, je v vsaj eni škatli več kot k žogic.

Lotimo se še malo zahtevnejših primerov:

Problem 1. *V sobi je 2017 oseb. Pokaži, da obstajata vsaj dve osebi, ki imata enako število znancev v sobi.*

Rešitev. Imejmo 2017 škatel, označenih s števili od 0 do 2016, in osebo spravimo v škatlo n , če ima v sobi natanko n znancev. Če je kakšna oseba v škatli številka 0, potem ni nikogar v škatli številka 2016, in obratno. Torej imamo v resnici na voljo 2016 škatel, kamor razporejamo 2017 oseb. Sedaj lahko neposredno uporabimo Dirichletov princip in sklepamo, da sta v eni od škatel vsaj dve osebi, to pa je ravno rešitev našega problema. $\square$

Problem 2. *Med n celimi števili vedno obstaja podmnožica teh števil, katere vsota je deljiva z n .*

Rešitev. Naj bodo $x_1, x_2, \dots, x_n$ cela števila. Oglejmo si vsote

$$\begin{aligned} s_1 &= x_1, \\ s_2 &= x_1 + x_2, \\ &\dots \\ s_n &= x_1 + x_2 + \dots + x_n. \end{aligned}$$

Če je že ena od teh vsot deljiva z n , potem je naloga rešena. V nasprotnem primeru vse vsote pri deljenju z n dajo neničeln ostanek. Teh vsot je n , na voljo pa imamo le $n - 1$ neničelnih ostankov. Po Dirichletovem principu obstajata dve vsoti, recimo s_m in s_{m+k} , ki pri deljenju z n dasta enak ostanek. Potem pa je vsota

$$s_{m+k} - s_m = x_{m+1} + x_{m+2} + \dots + x_{m+k}$$

deljiva z n . $\square$

Naslednje dejstvo se da izpeljati s pomočjo Evklidovega algoritma, tu pa pokažimo, kako do njega pridemo z Dirichletovim principom. Spomnimo se, da pravimo, da sta naravni števili m in n tuji, če je 1 največje naravno število, ki hkrati deli m in n .

Problem 3. *Naj bosta m in n tuji naravni števili. Potem obstajata naravni števili x in y , da je $nx - my = 1$.*

Rešitev. Oglejmo si števila $n, 2n, \dots, (m-1)n$ in njihove ostanke pri deljenju z m . Ker nobeno od navedenih števil ni deljivo z m , se ostanek 0 ne pojavi. Ali se lahko zgodi, da se tudi ostanek 1 ne pojavi? Če bi se to zgodilo, bi imeli na voljo $m-2$ vrednosti za ostanke in bi po Dirichletovem principu v zgornjem zaporedju števil obstajali dve različni števili, označimo ju z an in bn kjer je $a > b$, ki bi pri deljenju z m dali enak ostanek. V tem primeru bi bilo število $an - bn = (a-b)n$ deljivo z m , to pa ni mogoče, saj sta m in n tuji števili in $a-b < m$. Sklepamo torej, da obstaja naravno število $x \in \{1, 2, \dots, m-1\}$, da je ostanek nx pri deljenju z m enak 1, kar lahko zapišemo tudi kot $nx = my + 1$ za neki $y \in \mathbb{N}$. $\square$

Hitro lahko preverimo, da velja tudi obrat trditve v zgornjem primeru; če za naravni števili m in n obstajata naravni števili x in y , da je $nx - my = 1$, potem sta m in n tuji števili. Če je namreč največji skupni delitelj števil m in n enak d , potem lahko zapišemo $m = dm_1$ in $n = dn_1$ za neki naravni števili m_1 in n_1 in dobimo $d(n_1x - m_1y) = 1$, od koder takoj sledi $d = 1$.

Problem 4. *V ravnini je 2017 različnih točk, za katere velja, da v poljubni trojici točk obstajata dve, ki sta oddaljeni za manj kot 1. Pokaži, da obstaja krog s polmerom 1, znotraj katerega je vsaj 1009 točk.*

Rešitev. Naj bosta A in B takšni točki, za kateri je razdalja $|AB|$ največja možna. Če je $|AB| < 1$, je naloga že rešena; krog s središčem v A in polmerom 1 vsebuje v svoji notranjosti vseh 2017 danih točk. Predpostavimo torej, da je $|AB| \geq 1$. Če je X katerakoli od danih točk, ki je različna od A in B , potem velja $|AX| < 1$ ali $|BX| < 1$. V tem primeru vsaka od danih točk pade v notranjost kroga s središčem v A in polmerom 1 ali v notranjost

kroga s središčem B in polmerom 1. V jeziku škatel, v dve škatli razporejamo $2017 = 1008 \cdot 2 + 1$ žogic. Zato ena od škatel (torej eden od krogov) vsebuje več kot 1008 žogic (torej točk). $\square$

Bralca vabimo k rešitvi naslednjih nalog:

1. V kocki z robom dolžine 5 na slepo izberemo 124 točk. Pokaži, da znotraj te kocke obstaja kocka z robom dolžine 1, ki ne vsebuje nobene od izbranih točk.
2. V sobi je 2017 oseb, vsak se rokuje z vsakim. Potem sta v vsakem trenutku v sobi vsaj dve osebi, ki sta se do tega časa rokovali z enakim številom oseb.
3. V konveksnem šestkotniku vedno obstaja diagonala, ki odreže trikotnik, katerega ploščina ne presega ene šestine ploščine šestkotnika.
4. Naj bosta a in b tuji naravni števili. Potem v decimalnem zapisu ulomka a/b perioda decimalk ne presega $b - 1$.

Oglejmo si sedaj primer, ko razporejamo m žogic v n škatel. Če je $m \leq n$, se prav lahko zgodi, da nobena od škatel ne vsebuje več kot ene žogice. Lahko pa govorimo o *verjetnosti*, da vsaj ena od škatel vsebuje vsaj dve žogici. Formalne definicije verjetnosti tu ne bomo navedli, bodimo malce površni. Predstavljajmo si, da žogice na slepo mečemo v škatle, za nas pa bo zanimiv *dogodek*, da po koncu razporejanja vsaj ena škatla vsebuje vsaj dve žogici. Če z x označimo število načinov, na katere lahko m žogic razporedimo v n predalov, z y pa število tistih razporejanj, ki dajo ugoden rezultat, torej, da vsaj ena škatla vsebuje vsaj dve žogici, potem razmerju

$$p = \frac{y}{x}$$

pravimo *verjetnost* dogodka, da vsaj ena škatla vsebuje vsaj dve žogici. Število p torej pove razmerje med številom „dobrih razporejanj“ in številom vseh razporejanj žogic v škatle. Dirichletov princip pravi nič drugega kot to, da če razporejamo vsaj $n + 1$ žogic v n škatel, potem je $p = 1$. V teoriji verjetnosti pravimo, da je dogodek „v vsaj eni škatli sta vsaj dve žogici“ *gotov dogodek*.

Poskusimo izračunati verjetnost p v splošnem. Najprej si oglejmo, na koliko načinov lahko razporedimo m žogic v n škatel. Pri tem predpostavimo, da je $m \leq n$. Mislimo si, da žogice zaporedoma mečemo v škatle brez omejitev. Za prvo žogico imamo n možnih izbir škatle, za drugo prav tako itd. Za razporeditev m žogic v n škatel imamo torej na voljo $x = n^m$ razporejanj. Izračunajmo še y , pri čemer si pomagajmo z manjšim trikom. Oglejmo si namreč število $x - y$. To je ravno število vseh možnih razporejanj žogic v škatle, pri katerih na koncu vsaka škatla vsebuje *kvečjemu eno žogico*. V tem primeru imamo za prvo žogico n možnih izbir škatle. Za drugo žogico velja, da je ne smemo dati tja, kjer je že prva, torej imamo na voljo še $n - 1$ škatel. Podobno imamo za tretjo žogico $n - 2$ možnih izbir škatle. Na koncu imamo za m -to žogico natanko $n - m + 1$ možnih izbir škatle. Zato je $x - y = n(n - 1)(n - 2) \cdots (n - m + 1)$, torej dobimo

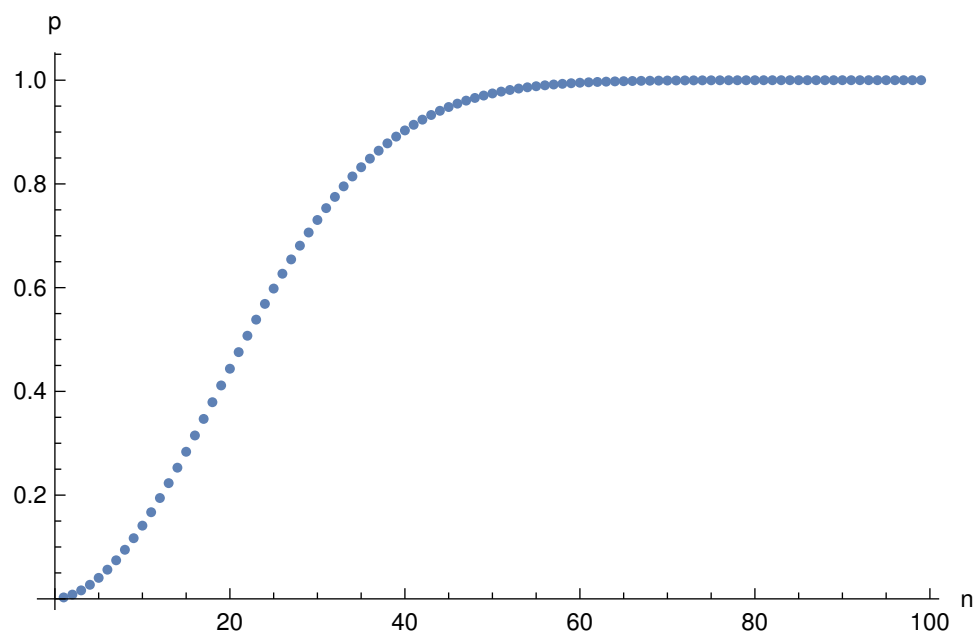
$$\begin{aligned} p &= \frac{n^m - n(n - 1)(n - 2) \cdots (n - m + 1)}{n^m} \\ &= 1 - \frac{n(n - 1)(n - 2) \cdots (n - m + 1)}{n^m}. \end{aligned}$$

Opazimo, da formula velja tudi za primer, ko je $m > n$. V tem primeru je namreč števec drugega ulomka v zgornjem izrazu enak 0 in je $p = 1$, kar je ravno Dirichletov princip.

Recimo, da imamo skupino n ljudi in gledamo njihove rojstne dneve. Zaradi enostavnosti predpostavimo, da je vsak od 365 dni neprestopnega leta enako verjeten kot rojstni dan, 29. februarja pa ne štejemo. Verjetnost, da imata vsaj dve osebi enak rojstni dan, je

$$p = 1 - \frac{365 \cdot 364 \cdots (366 - n)}{365^n}.$$

Na Sliki 2 je grafično prikazano, kako se p obnaša v odvisnosti od n . Rezultat je nekoliko presenetljiv. Za $n = 23$ dobimo $p = 0,507$, kar lahko interpretiramo kot dejstvo, da v skupini 23 ljudi obstaja 50 odstotna možnost, da imata vsaj dva enak rojstni dan. Ko je v skupini 60 ljudi, je ta možnost že 99,4 odstotna. To je v nasprotju z intuicijo, saj je ljudi le 60, možnih rojstnih dni pa 365, zato bi pričakovali, da je možnost, da imata vsaj dva med njimi enak rojstni dan, bistveno manjša. Temu navideznemu protislovju pravimo



Slika 2: Verjetnost, da imata med n ljudmi vsaj dve osebi isti rojstni dan.

paradoks rojstnega dneva, pojav pa se s pridom uporablja v kriptografiji pri naključnem razvozlanju šifriranih sporočil.

Bralec se lahko za konec pozabava z naslednjim problemom: Recimo, da ljudje vstopajo v sobo eden za drugim. Za katero osebo po vrsti bo verjetnost, da je prvi od ljudi, ki so vstopili, in ima enak rojstni dan kot nekdo, ki je že v sobi, največja?

Literatura

- [1] Dragoljub M. Milošević, prevod Peter Šemrl, *Dirichletov princip*, Presek **14** (1986 / 1987), številka 2, 110–111.